Welcome to the PIA for FY 2011!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508.

b. Records Officer is responsible for supplying records retention and deletion schedules.

c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.

d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.

e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect indentify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

Microsoft Office 2003: To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

Final Signatures

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

Privacy Impact Assessment Uploaded into SMART

Privacy Impact Assessments should be uploaded into C&A section of SMART.
All PIA Validation Letters should be emailed to christina.pettit@va.gov to received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name:	Region 3 > VHA > VISN 10 > Chillicothe VAMC > VISTA-VMS
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-01-11-01-1180-00
Description of System/ Application/ Program:	See section 1.8 General Purpose and Description in the System Security Plan found in SMART: The Department of Veterans Affairs (VA) has had automated information systems in its medical facilities since 1985, beginning with the Decentralized Hospital Computer Program information system, including extensive clinical and administrative capabilities. The Veterans Health Information Systems and Technology Architecture (VistA), supporting ambulatory and inpatient care, delivered significant enhancements to the original system with the release of the Computerized Patient Record System (CPRS) for clinicians in 1997. CPRS provides a single interface for health care providers to review and update a patient's medical record and to place orders, including medications, special procedures, x-rays, patient care nursing orders, diets, and laboratory tests. CPRS is flexible enough to be implemented in a wide variety of settings for a broad spectrum of health care workers and provides a consistent, event driven, Windows-style interface.
Facility Name:	Chillicothe VA Medical Center

Title:	Name:	Phone:	Email:
Privacy Officer:	Annette Damico	740-773-1141 e	annette.damico@va.gov
Information Security Officer:	Robert Barnhart	740-773-1141 e	Robert.Barnhart@va.gov
System Owner/ Chief Information Officer:	Lay, Michael R3 Director		Michael.Lay@va.gov
Information Owner:			
Other Titles:	Gawler, William C. FCIO	740-773-1141 e	William.Gawler@va.gov
Person Completing Document:			
Other Titles:	Janet Wallace, Manager, Customer Solutions & Support	740-773-1141 e	Janet.Wallace@va.gov
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)			04/2010 Validation Letter
Date Approval To Operate Expires:			08/2011

What specific legal authorities authorize this program or system:	Title 38, U.S.C, section 7301(a), Functions of Veterans Hea
What is the expected number of individuals that will have their PII stored in this system:	1-250,000
Identify what stage the System / Application / Program is at:	Operations/Maintenance
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	Year 1997
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes

If No, please explain:

Has a PIA been completed within the last three years?	Yes
Date of Report (MM/YYYY):	02/2011

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

- ☐ Have any changes been made to the system since the last PIA?
- ☑ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☑ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☑ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☑ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please complete TAB 7 & TAB 12. (See Comment for Definition of PII)

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.

For each applicable System(s) of Records, list:

1. All System of Record Identifier(s) (number):

2. Name of the System of Records:
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Does the System of Records Notice require modification or updating?

Is PII collected by paper methods?
Is PII collected by verbal methods?
Is PII collected by automated methods?
Is a Privacy notice provided?
Proximity and Timing: Is the privacy notice provided at the time of data collection?
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

Yes

79VA19
Veterans Health Information Systems and Technology Architecture (VISTA) Records

http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm

Yes

No

(Please Select Yes/No)

Yes

Yes

Yes

Yes

No

Yes

Yes

Yes

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	Veterans will receive Privacy Notice which explains use of data.	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	That the information is for emergency contacts, patient care issues and they are given the choice to "opt out".	Verbal & Written
Service Information	ALL	That it is used for determining eligibility and determining enrollment priority.	Verbal & Written
Medical Information	ALL	Used for continuity of care	Verbal & Written
Criminal Record Information	ALL	Compliance with Federal law, Fugitive Felon Program	Verbal & Written
Guardian Information	ALL	Required for release of information and consent for patient treatment.	Verbal & Written
Education Information	ALL	Credentialing and Privileging, Qualification determination, Clinical Trainee Information	Verbal & Written
Benefit Information	ALL	Classifying eligibility, determination of survivor benefits	Verbal & Written
Other (Explain)			

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Mandatory
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory
Medical Information	Yes	Other (Explain)	Mandatory
Criminal Record Information	Yes		
Guardian Information	Yes	Other (Explain)	Mandatory
Education Information	Yes	Other (Explain)	Mandatory
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory
Other (Explain)			
Other (Explain)			
Other (Explain)			

How is a privacy notice provided?
Written
Written
Written
Written
Written
Written
Written
Written

Additional Comments

If eligibility is based on finance, this information is considered mandatory for determination of eligibility

History is generally received during the patient interview, however additional medical records may come from Private Sector facilities and/or other VA Medical Centers

Legal representative

This may come from a variety of sources for determining qualification based on education

Veterans Benefits Administration; Social Security Administration; Health Eligibility Center; DOD

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VBA; Readjustment Counseling; Regional Counsel; Austin Automation Center; Denver Distribution Center;CMOP;Consolidated Patient Accounting Center	Yes	VBA/Regional Office: treatment and demographic for benefits determination. Regional Council: Tort Claims, legal processes. BAA in place. AAC - Workload, Fiscal, Claims; DDC - In conjunction with Prosthetics for issuance of certain Prosthetic items, eg. hearing aids; pressure socks, etc.; CMOP - RX and demographic information mailed out to patients; NPPD - Treatment, Benefits, Administrative	Both PII & PHI	VHA Handbook 1605.1, Policy Memo 161-10, Release of Information
Other Veteran Organization	Veteran Service Organizations	Yes	Read Only for Claims assistance	Both PII & PHI	VHA Handbook 1605.1, Policy Memo 161-10, Release of Information
Other Federal Government Agency	FBI ,OPM, DEA, DOD, Centers for Disease Control, Social Security Administration, Internal Revenue	Yes	Congressional inquiries accompanied by patient authorization; various information including appointment dates, treatment, medical documentation, bills, co-pays. There is certain VA patient data that is shared with DoD through the information exchange programs. In addition, certain clinical data is shared with CDC.	Both PII & PHI	VHA Handbook 1605.1, Policy Memo 161-10, Release of Information

State Government Agency	State Police, Ohio Bureau of Motor Vehicles, Dept. of Health, Ohio Dept. of Job and Family Services	No	Per standing letters: BMV, HHS, Job & Family Services	Both PII & PHI	VHA Handbook 1605.1, Policy Memo 161-10, Release of Information
Local Government Agency	Local Police; County Coronor	No	Assist with investigations and completion of death certificates	Both PII & PHI	VHA Handbook 1605.1, Policy Memo 161-10, Release of Information
Research Entity	VA Internal - Cincinnati VAMC IRB	Yes	Research studies/protocols	Both PII & PHI	VHA Handbook 1200.01, Research and Development VHA Handbook 1200.05, Requirements for the Protection of Human Subject Monitoring
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system?		Yes
Please enter the name of the system:	VBA, Clinical Applications, eg. Vista Imaging, Clinical Procedures, IMED Consent, DOD,	
Per responses in Tab 4, does the system gather information from an individual?		Yes
If information is gathered from an individual, is the information provided:	☑ Through a Written Request ☑ Submitted in Person ☑ Online via Electronic Form	
		Yes
Is there a contingency plan in place to process information when the system is down?		Yes

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?	Yes

☑ Drug/Alcohol Counseling ☑ Mental Health ☑ HIV

☑ Research ☐ Other (Please Explain)

☑ Sickle Cell

if yes, please check all that apply:

Describe process for authorizing access to this data.

Answer: Requirements for the Protection of Human Subjects in Research VHA Handbook 1200.05 and 7332 information is by VA 10-5345 Authorization to Release.

(FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public? No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Standardized VA forms, Limitations within Vista Applications, Access Limitations (Minimum Necessary/Functional Category)of users.

How is data checked for completeness?

Answer: Manually as well as input validation within the Vista software to ensure data integrity

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer: Policy Memo updates; Standard Operating Procedures and VA Directives;HEC Notifications

How is new data verified for relevance, authenticity and accuracy?

Answer: Manually and through automatic means through Austin when data is rejected

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Medical Records are retained 75 years after the last episode of care. All other data is based on Records Control Schedule RCS10-1 and National Archives Records Administration

Explain why the information is needed for the indicated retention period?

Answer: Mandated by policy

What are the procedures for eliminating data at the end of the retention period?

Answer: Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XLIII, 2.b. (Page 190). At the present time, VistA Imaging retains all images. We are performing a study to explore whether some images can be eliminated on an earlier schedule.

Where are these procedures documented?

Answer: VA Records Control Schedule 10-1 (page 8): Records Management Responsibilities
The Health Information Resources Service (HIRS) is responsible for developing policies and procedures for effective and efficient records management throughout VHA. In addition, HIRS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices and procedures.
Field records officers are responsible for records management activities at their facilities.
Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with NARA regulations and VA policy.
All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures.
Disposition of Records

How are data retention procedures enforced?
Answer: Records Control Manager

Has the retention schedule been approved by the National Archives and Records Administration (NARA)	Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)
Answer: IT Media Backup requirements are consistent with RCS 10 requirements for data retention.

(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?	No

If Yes, How will parental or guardian approval be obtained?
Answer:

(FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	Yes
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	Yes
Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	No
Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	No
Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	

If 'No' to any of the 3 questions above, please describe why:

Answer: SCA testing is a 3 year requirement unless there is a significant change, while continuous monitoring is annual during the off years that the SCA is not conducted. Risk assessments are reviewed annually and completed every 3 years, unless there is a significant change to the system, e.g. new hardware/software platform.

Is adequate physical security in place to protect against unauthorized access?	Yes

If 'No' please describe why:

Answer:

Explain how the project meets IT security requirements and procedures required by federal law.

Answer: The agency is following IT security requirements as described in the FISMA and as implemented by VA Handbook 6500. IT security measures include implementation of the High-baseline of management, technical and operational security controls from NIST Special Publication 800-53, Rev 3. Security control assessments are conducted at least annually.

Explain what security risks were identified in the security assessment? *(Check all that apply)*

- [x] Air Conditioning Failure
- [x] Chemical/Biological Contamination
- [ ] Blackmail
- [ ] Bomb Threats
- [x] Burglary/Break In/Robbery
- [x] Cold/Frost/Snow
- [ ] Communications Loss
- [x] Computer Intrusion
- [x] Data Disclosure
- [ ] Data Integrity Loss
- [ ] Denial of Service Attacks
- [ ] Earthquakes
- [x] Eavesdropping/Interception
- [x] Errors (Configuration and Data Entry)
- [x] Fire (False Alarm, Major, and Minor)
- [x] Flooding/Water Damage
- [x] Hardware Failure
- [x] Identity Theft
- [x] Malicious Code
- [x] Power Loss
- [x] Sabotage/Terrorism
- [x] Storms/Hurricanes
- [ ] Substance Abuse
- [x] Theft of Assets

- [x] Computer Intrusion
- [x] Computer Misuse
- [x] Data Destruction
- [x] Fire (False Alarm, Major, and Minor)
- [x] Flooding/Water Damage
- [ ] Fraud/Embezzlement
- [x] Theft of Assets
- [x] Theft of Data
- [x] Vandalism/Rioting

Answer: (Other Risks) Component Failure; Indoor Humidity; Civil Unrest; Hacker/Cracker; Human Health Emergency (e.g. Pandemic); Unavailability of Personnel; Negligence

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

- ☑ Access Control
- ☑ Audit and Accountability
- ☑ Awareness and Training
- ☑ Certification and Accreditation Security Assessments
- ☑ Configuration Management
- ☑ Contingency Planning
- ☑ Identification and Authentication
- ☑ Incident Response
- ☑ Media Protection
- ☑ Personnel Security
- ☑ Physical and Environmental Protection
- ☑ Risk Management

Answer: (Other Controls) Privacy;

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.
Answer: No new findings following the previous PIA, therefore, no additional considerations for any of the security controls and/or policies needed at this time.

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. ☐ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. ☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑ The potential impact is **high** if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. ☐ The potential impact is **moderate** if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals. ☐ The potential impact is **low** if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.
Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon	☑ The potential impact is **high** if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. ☐ The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.

the system or organization?	**(Choose One)**	☐	The potential impact is **low** if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2011) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?

Access Manager
Actuarial
Appraisal System
ASSISTS
Awards
Awards
Baker System
Bbraun (CP Hemo)
BDN Payment History
BIRLS
C&P Payment System
C&P Training Website
CONDO PUD Builder
Corporate Database
Data Warehouse
EndoSoft
FOCAS
Inforce
INS - BIRLS
Insurance Online
Insurance Self Service
LGY Home Loans
LGY Processing
Mobilization
Montgomery GI Bill
MUSE
Omnicell
Priv Plus
RAI/MDS
Right Now Web
SAHSHA
Script Pro
SHARE
SHARE
SHARE
Sidexis
Synquest

Automated Sales Reporting (ASR)
BCMA Contingency Machines
Benefits Delivery Network (BDN)
Centralized Property Tracking System
Common Security User Manager (CSUM)
Compensation and Pension (C&P)
Control of Veterans Records (COVERS)
Control of Veterans Records (COVERS)
Control of Veterans Records (COVERS)
Courseware Delivery System (CDS)
Dental Records Manager
Education Training Website
Electronic Appraisal System
Electronic Card System (ECS)
Electronic Payroll Deduction (EPD)
Eligibility Verification Report (EVR)
Fiduciary Beneficiary System (FBS)
Fiduciary STAR Case Review
Financial and Accounting System (FAS)
Insurance Unclaimed Liabilities
Inventory Management System (IMS)
LGY Centralized Fax System
Loan Service and Claims
Loan Guaranty Training Website
Master Veterans Record (MVR)
Mental Health Asisstant
National Silent Monitoring (NSM)
Powerscribe Dictation System
Rating Board Automation 2000 (RBA2000)
Rating Board Automation 2000 (RBA2000)
Rating Board Automation 2000 (RBA2000)
Records Locator System
Review of Quality (ROQ)
Search Participant Profile (SPP)
Spinal Bifida Program Ch 18
State Benefits Reference System
State of Case/Supplemental (SOC/SSOC)

Automated Folder Processing System (AFPS)
Automated Medical Information Exchange II (AIME II)
Automated Medical Information System (AMIS)290
Automated Standardized Performace Elements Nationwide (ASPEN)
Centralized Accounts Receivable System (CARS)
Committee on Waivers and Compromises (COWC)
Compensation and Pension (C&P) Record Interchange (CAPRI)
Compensation & Pension Training Website
Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
Distribution of Operational Resources (DOOR)
Educational Assistance for Members of the Selected Reserve Program CH 1606
Electronic Performance Support System (EPSS)
Enterprise Wireless Messaging System (Blackberry)
Financial Management Information System (FMI)
Hearing Officer Letters and Reports System (HOLAR)
Inquiry Routing Information System (IRIS)
Modern Awards Process Development (MAP-D)
Personnel and Accounting Integrated Data and Fee Basis (PAID)
Personal Computer Generated Letters (PCGL)
Personnel Information Exchange System (PIES)
Personnel Information Exchange System (PIES)
Post Vietnam Era educational Program (VEAP) CH 32
Purchase Order Management System (POMS)
Reinstatement Entitelment Program for Survivors (REAPS)
Reserve Educational Assistance Program CH 1607
Service Member Records Tracking System
Survivors and Dependents Education Assistance CH 35
Systematic Technical Accuracy Review (STAR)
Training and Performance Support System (TPSS)
VA Online Certification of Enrollment (VA-ONCE
VA Reserve Educational Assistance Program
Veterans Appeals Control and Locator System (VACOLS)
Veterans Assistance Discharge System (VADS)
Veterans Exam Request Info System (VERIS)
Veterans Service Representative (VSR) Advisor
Vocational Rehabilitation & Employment (VR&E) CH 31
Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

VBA Data Warehouse	Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)
Web LGY		Work Study Management System (WSMS)

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

- X ASISTS
- Bed Control
- X CAPRI
- X CMOP
- X Dental
- X Dietetics
- X Fee Basis
- GRECC
- X HINQ
- X IFCAP
- X Imaging
- X Kernal
- X Kids
- X Lab Service
- Letterman
- X Library
- X Mailman
- X Medicine
- MICOM
- NDBI
- X NOIS
- X Oncology
- X PAID
- X Prosthetics
- X QUASAR
- X RPC Broker
- X SAGG
- X Scheduling
- X Social Work
- X Surgery
- Toolkit
- Unwinder
- X VA Fileman
- X VBECS
- VDEF
- VistALink
- X Beneficiary Travel
- X Care Management
- Care Tracker
- X Clinical Reminders
- X CPT/ HCPCS Codes
- X DRG Grouper
- X DSS Extracts
- X Education Tracking
- X Engineering
- X Event Capture
- Extensible Editor
- X Health Summary
- Incident Reporting
- X Intake/ Output
- X Integrated Billing
- X Lexicon Utility
- X List Manager
- X Mental Health
- X MyHealthEVet
- X National Drug File
- X Nursing Service
- Occurrence Screen
- X Patch Module
- Patient Feedback
- Police & Security
- Problem List
- Progress Notes
- X Record Tracking
- X Registration
- Run Time Library
- Survey Generator
- X Utilization Review
- Visit Tracking
- VistALink Security
- X Women's Health
- X Accounts Receivable
- ADP Planning (PlanMan)
- X Bar Code Med Admin
- Clinical Case Registries
- X Clinical Procedures
- X Consult/ Request Tracking
- X Controlled Substances
- X Credentials Tracking
- X Discharge Summary
- X Drug Accountability
- X EEO Complaint Tracking
- X Electronic Signature
- Event Driven Reporting
- X External Peer Review
- X Functional Independence
- Gen. Med. Rec. - I/O
- X Gen. Med. Rec. - Vitals
- X Generic Code Sheet
- X Health Level Seven
- X Hospital Based Home Care
- X Inpatient Medications
- X Integrated Patient Funds
- MCCR National Database
- Minimal Patient Dataset
- X National Laboratory Test
- X Network Health Exchange
- X Outpatient Pharmacy
- X Patient Data Exchange
- X Patient Representative
- X PCE Patient/ HIS Subset
- Security Suite Utility Pack
- Shift Change Handoff Tool
- X Spinal Cord Dysfunction
- X Text Integration Utilities
- VHS & RA Tracking System
- X Voluntary Timekeeping
- X Adverse Reaction Tracking
- Authorization/ Subscription
- Auto Replenishment/ Ward Stock
- Automated Info Collection Sys
- X Automated Lab Instruments
- X Automated Med Info Exchange
- Capacity Management - RUM
- Capacity Management Tools
- Clinical Info Resource Network
- X Clinical Monitoring System
- X Enrollment Application System
- X Equipment/ Turn-in Request
- Gen. Med.Rec. - Generator
- X Health Data and Informatics
- ICR - Immunology Case Registry
- X Income Verification Match
- X Incomplete Records Tracking
- Interim Mangement Support
- X Master Patient Index VistA
- X Missing Patient Reg (Original) A4EL
- X Order Entry/ Results Reporting
- X PCE Patient Care Encounter
- X Pharmacy Benefits Mangement
- X Pharmacy Data Management
- Pharmacy National Database
- X Pharmacy Prescription Practice
- X Quality Assurance Integration
- X Quality Improvement Checklist
- X Radiology/ Nuclear Medicine
- X Release of Information - DSSI
- X Remote Order/ Entry System
- X Utility Management Rollup
- CA Vertified Components - DSSI
- Vendor - Document Storage Sys
- X Visual Impairment Service Team ANRV
- Voluntary Timekeeping National

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web	ENDSOFT	RAFT
	Enterprise Terminology Server &	RALS
A4P	VHA Enterprise Terminology Services	

(FY 2011) PIA: Final Signatures

Facility Name: Region 3 > VHA > VISN 10 > Chillicothe VAMC > VISTA-VMS

Title:	Name:	Phone:	Email:
Privacy Officer:	Annette Damico	740-773-1141 ext 7020	annette.damico@va.gov
Digital Signature Block			
Information Security Officer:	Robert Barnhart	740-773-1141 ext 7071	Robert.Barnhart@va.gov
Digital Signature Block			
System Owner/ Chief Information Officer:	Lay, Michael R3 Director	0	Michael.Lay@va.gov
Digital Signature Block			
Information Owner:	0	0	0
Digital Signature Block			
Other Titles:	Gawler, William C. FCIO	740-773-1141 ext 7007	William.Gawler@va.gov
Digital Signature Block			

Date of Report: 1/0/00

OMB Unique Project Identifier 029-00-01-11-01-1180-00

Project Name	Region 3 > VHA > VISN 10 > Chillicothe VAMC > VISTA-VMS

(FY 2011) PIA: Final Signatures

Facility Name: Region 3 > VHA > VISN 10 > Chillicothe VAMC > VISTA-VMS

Title:	Name:	Phone:	Email:
Privacy Officer:	Annette Damico	740-773-1141 ext 7020	annette.damico@va.gov
	Annette M Damico 3/9/11		
Information Security Officer:	Robert Barnhart	740-773-1141 ext 7071	Robert.Barnhart@va.gov
	Robert W Barnhart 3/9/2011		
System Owner/ Chief Information Officer:	Lay, Michael R3 Director	0	Michael.Lay@va.gov
Information Owner:	0	0	0
Other Titles:	Gawler, William C. FCIO	740-773-1141 ext 7007	William.Gawler@va.gov
	William C. Gawler		
Date of Report:	1/0/00		
OMB Unique Project Identifier	029-00-01-11-01-1180-00		